



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Matthew Conover, Peter Szor

Assignee: Symantec Corporation

RETURN-TO-LIBC ATTACK DETECTION USING BRANCH

TRACE RECORDS SYSTEM AND METHOD

Serial No.:

10/763,867

Filed:

January 22, 2004

2131

Examiner:

Title:

Unknown

Group Art

Unit:

Docket No.:

SYMC1044

Monterey, CA May 18, 2004

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant(s) wish to call the following documents (a copy of each is enclosed) to the attention of the Examiner.

U.S. PATENT DOCUMENTS

\	DOCUMENT NUMBER	DATE	NAME				
1)	5,822,517	10/13/1998	Dotan				
2)	6,301,699	10/09/2001	Hollander et al.				

OTHER DOCUMENTS

1)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
2)	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: URL:http://www.windowsitlibrary.com/Content/356/06/2.html.
3)	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: kernelmode.asp="" products="" technology="" www.entercept.com="">. No author provided.</url:http:>
4)	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: interception.asp="" products="" technology="" www.entercept.com="">. No author provided.</url:http:>
5)	Gordon, J., "Understand the Stack (part 1)", pp. 1-8 [online]. Retrieved on August 27, 2003. Retrieved from the Internet: <url:http: goasmhelp="" usstack1.htm="" www.jorgon.freeserve.co.uk=""></url:http:>
6)	Chew, M. and Song, D., "Mitigating Buffer Overflows by Operating System Randomization", December 2002, 9 pages.
7)	"Entercept Continues to Dominate the Market in Buffer Overflow Protection", pg. 1-2 [online]. Retrieved on August 6, 2003. Retrieved from the Internet: <url:http: 07-09-02.asp="" news="" uspr="" www.entercept.com="">. No author provided.</url:http:>
8)	"IA-32 Intel® Architecture Software Developer's Manual; Volume 3: System Programming Guide", pgs. 15-11 to 15-22. 2002. No author provided.
9)	Dabak, P., Borate, M., Phadke, S., Adding New System Services to the Windows NT Kernal", pp. 1-5 [online]. Retrieved December 16, 2003. Retrieved from the Internet: URL: http://www.windowsitlibrary.com/Content/356/07/1.html.
10)	Szor, U.S. Patent Application Serial No. 10/671,202, filed September 25, 2003, entitled "RETURN-TO-LIBC ATTACK BLOCKING SYSTEM AND METHOD".
11)	Szor, U.S. Patent Application Serial No. 10/360,341, filed February 6, 2003, entitled "SHELL CODE BLOCKING SYSTEM AND METHOD".
12)	Sobel et al., U.S. Patent Application Serial No. 10/140,149, filed May 6, 2002, entitled "ALTERATION OF MODULE LOAD LOCATIONS".

A PTO form 1449 listing these documents is enclosed. Citation of the above documents shall not be construed as:

- 1. an admission that the documents are necessarily prior art with respect to the instant invention;
- a representation that a search has been made,
 other than as described above; or
- 3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as First Class Mail in an envelope addressed to: Commissioner for Patents, P.Q. Box 1450, Alexandria, VA 22313-1450, on

May 18, 2004.

Attorney for Applicant(s)

May 18, 2004
Date of Signature

Respectfally submitted,

Serge J. Hødgson

Attorney fbr Applicant(s)

Reg. No. 40,017 (831) 655-0880

Form PTO-1449	Atty Docket No.	Serial No.				
PEJC	SYMC1044	10/763,867				
PE CONTRACTION DISCLOSURE CITATION IN AN APPLICATION	Applicant(s)					
10 IN AN APPLICATION	Matthew Conover et al.					
With the second	Filing Date	Group				
MAT (Use several sheets if necessary)	January 22, 2004	2131				

			U.S.	PATENT DOCUMENTS		-					
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING I				
	AA	5,822,517	10/13/1998	Dotan	395	186					
	AB	6,301,699	10/09/2001	Hollander et al.	717	4					
_	AC										
	AD										
	AE										
-	AF										
	AG										
•	AH										
	AI										
	AJ										
	AK					-					
·	<u> </u>		FOREI	GN PATENT DOCUMENTS	3		·				
							Trans	lation			
•		DOCUMENT NUMB	R DATE	COUNTRY	CLASS	SUBCLASS	YES	NO			
	AL										
	AM										
	AN										
	AO										
	AP										
		OTHER DOCUM	ENTS (Includir	ng Author, Title, Date,	Pertinent P	ages, Etc.)	•				
	AR	Buffer-Over Conference,	flow Techniq	"Blended Attacks I ues In Computer Vi 002, Virus Bulletin p. 1-36.	ruses", Vi	rus Bulle	tin				
	AS	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet:									
	AT	from the Internet: URL:http://www.windowsitlibrary.com/Content/356/06/2.html. "How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: kernelmode.asp="" products="" technology="" www.entercept.com="">. No author provided.</url:http:>									

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Form PTO-1449					Atty Dock	et No.		Serial No.			
						SYMC104	4		10/763,	867	
	INFOR	MATION DISCI	osu	RE CITATI	ION	Applicant(s)					
		IN AN APPI	ICA	TION		Matthew Conover et al.					
						Filing Da	te	Group	Group		
(Use several sheets if necessary)				January	22, 2004	"	2131				
	1	T =======	<u> </u>	U. 8	S. PATENT DO	OCUMENTS			——————————————————————————————————————		
EXAMINER INITIAL	177075			DATE NAME		CLASS		ASS SUBCLASS		S FILING DATE IF APPROPRIATE	
	AA		_			<u>-</u>					
	AB		_								
	AC					<u> </u>					
	AD										
	AE										
	AF										
	AG										
	AH										
	AI										
	AJ										
	AK					-					
				FORE	IGN PATENT	DOCUMENTS	5				
									Tran	slation	
		DOCUMENT NUME	BER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	NO	
	AL										
	AM										
	AN										
	AO										
	AP		.,								
		OTHER DOCU	MENT	S (Includ	ing Author, Ti	tle, Date,	Pertinent P	ages, Etc.	.)		
	AR	Retrieved	on A	April 16, ww.enterc	s: System 2003. Ret ept.com/pro	rieved f	rom the In	ternet:			
	AS Gordon, J., "Understand the Stack Retrieved on August 27, 2003. Retrieved.http://www.jorgon.freeserve.co						etrieved from the Internet:				
	AT	Chew, M. a Randomizat	nd S ion'	Song, D., ", Decemb	"Mitigatin er 2002, 9	g Buffer pages.	Overflows	by Ope.	rating S	ystem	
Examiner			1	Date Cons	sidered						
EXAMINER: through ci to applica	tation	al if reference if not in con	e con	nsidered, when the same and not are as a second not as a second not are a second not a second not are a second not are a second not a sec	hether or not t considered.	citation is Include co	s in conformation of this :	ance with form with	MPEP 609; next comm	draw line	

Form PTO-1449					Atty Dock	et No.	Serial No	.				
						SYMC104	4		10/763,	867		
	INFORM	MATION DISC	Losu	RE CITATIO	ON	Applicant(s)						
		IN AN APP	LICA	rion		Matthew Conover et al.						
						Filing Da	ite		Group			
	(Use several sheets if necessary)						22, 2004		2131			
		·		U.S	. PATENT D	DOCUMENTS						
EXAMINER INITIAL		DOCUMENT NUMBER	DA	.TE	NAME		CLASS	SUBCLASS		DATE PROPRIATE		
	AA											
	AB											
	AC											
	AD											
	AF		\top									
	AF											
	AG											
	AH											
	AI											
	AJ		1				1					
	AK		1									
				FOREI	GN PATENT	DOCUMENT	s					
									Tran	slation		
		DOCUMENT NUM	BER	DATE	COUNTRY		CLASS	SUBCLASS	S YES	мо		
	AL				•							
		·										
	AM			<u> </u>	1			l				
	AM AN											
	 											
	AN											
	AN AO	OTHER DOCU	MENT	S (Includi	ing Author, T	itle, Date,	Pertinent	Pages, Etc.	.)			
	AN AO	"Entercept Protection	t Con	ntinues to og. 1-2 [c	ing Author, To Dominate online]. In the continuity of the continui	the Mark Retrieved	et in Buf l on Augus	fer Overs	flow 3. Retr	ieved 2.asp>.		
	AN AO AP	"Entercept Protection from the I No author	t Con n", p Inter c pro	ntinues to og. 1-2 (c rnet: <uri ovided. Architec</uri 	o Dominate	the Mark Retrieved ww.enterc	et in Buf l on Augus ept.com/n	fer Overi t 6, 2003 ews/uspr/	flow 3. Retr /07-09-0	2.asp>. System		
	AN AO AP	"Entercept Protection from the I No author "IA-32 Int Programmin Dabak, P., Windows NI Retrieved	t Con ", p Inter c pro tel® ng Gu Bor F Ker from	atinues to og. 1-2 [cret: <uri ovided. Architectide", pgs cate, M., cnal", pp.</uri 	o Dominate online]. I b:http://ww ture Softw s. 15-11 to Phadke, S . 1-5 [onl:	the Mark Retrieved www.enterc vare Devel o 15-22, Adding ine]. Ret	tet in Buf l on Augus ept.com/n loper's Ma 2002. No New Syst rieved De	fer Overit 6, 2003 ews/uspr/ anual; Vo. author pr em Servic cember 16	flow 3. Retr /07-09-0	2.asp>. System he		

Form PTO-1449					Atty Docket No. Serial No.							
					SYMC1044 10/763,867							
]	INFORMATION DISCLOSURE CITATION					Applicant(s)						
IN AN APPLICATION (Use several sheets if necessary)					Matthew Conover et al.							
					Filing Dat	:е		Gr	roup			
					January	22, 2004		2:	131			
			OCUMENTS									
EXAMINER INITIAL		DOCUMENT NUMBER				CLASS SUBG			JBCLASS FILING DATE IF APPROPRIATE			
	AA											
	AB											
	AC											
	AD											
	AE											
	AF											
	AG								\neg			
	AH											
	AI											
	AJ								\neg			
	AK											
				FOREIG	N PATENT	DOCUMENTS	<u>. </u>	<u> </u>				
-				•						Transl	ation	
		DOCUMENT NUMBE	R	DATE	COUNTRY		CLASS	SUBCLAS	s	YES	NO	
	AL		ヿ									
	AM								\neg			
	AN	-	\dashv									
	AO		_						\neg			
	AF								\exists			
		OTHER DOCUM	ENT!	S (Including	l g Author, Ti	itle, Date,	Pertinent Pa	ges, Etc.	 .)			
	AR Szor, U.S. Patent Application Serial No. 10/671,202, filed September 25 2003, entitled "RETURN-TO-LIBC ATTACK BLOCKING SYSTEM AND METHOD".									25,		
	AS Szor, U.S. Patent Application Serial No. 10 2003, entitled "SHELL CODE BLOCKING SYSTEM							, filed DD".	Fe	bruary	6,	
	АТ	Sobel et al 2002, entit	., U	U.S. Paten "ALTERATI	nt Applica ION OF MOD	tion Seri DULE LOAD	al No. 10, LOCATIONS'	/140,149	9,	filed M	ay 6,	
Examiner			D	ate Consid	dered							
EXAMINER: through cit to applicat	tation	al if reference if not in confo	cons	sidered, whet nce and not o	ther or not considered.	citation is Include co	in conforma	nce with orm with	MPE	P 609; dr	aw line cation	